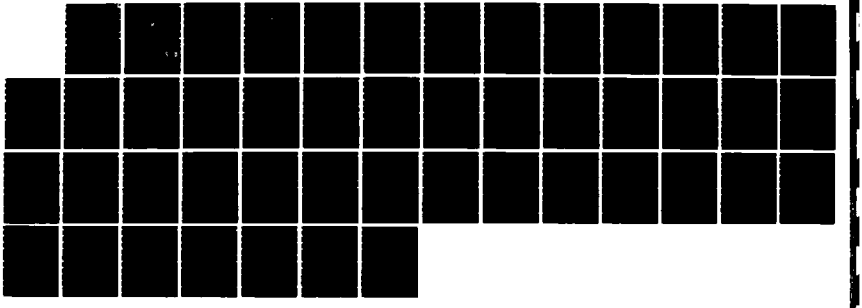
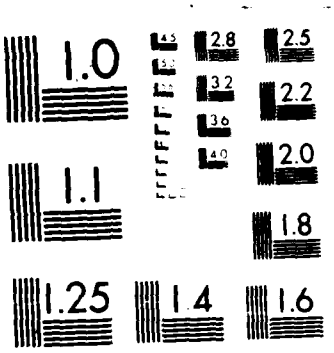
AD-A179 842 TECHNOLOGY TRANSFER - ITS IMPLICATIONS FOR DOD(U) AIR 1/1
COMMAND AND STAFF COLL MAXWELL AFB AL T N WANG APR 87
ACSC-87-2645

UNCLASSIFIED F/G 5/2 NL





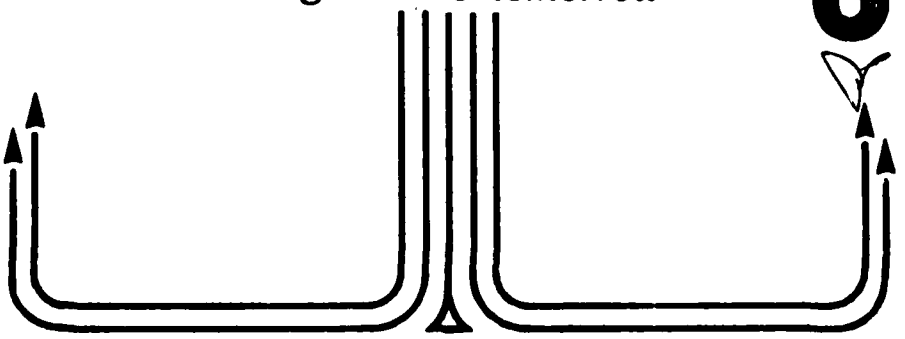
AIR COMMAND AND STAFF COLLEGE

STUDENT REPORT

TECHNOLOGY TRANSFER--ITS IMPLICATIONS FOR DOD

MAJOR TEDDY N. WANG 87-2645

"insights into tomorrow"



DISCLAIMER

The views and conclusions expressed in this document are those of the author. They are not intended and should not be thought to represent official ideas, attitudes, or policies of any agency of the United States Government. The author has not had special access to official information or ideas and has employed only open-source material available to any writer on this subject.

This document is the property of the United States Government. It is available for distribution to the general public. A loan copy of the document may be obtained from the Air University Interlibrary Loan Service (AUL/LDEX, Maxwell AFB, Alabama, 36112) or the Defense Technical Information Center. Request must include the author's name and complete title of the study.

This document may be reproduced for use in other research reports or educational pursuits contingent upon the following stipulations:

-- Reproduction rights do not extend to any copyrighted material that may be contained in the research report.

-- All reproduced copies must contain the following credit line: "Reprinted by permission of the Air Command and Staff College."

-- All reproduced copies must contain the name(s) of the report's author(s).

-- If format modification is necessary to better serve the user's needs, adjustments may be made to this report--this authorization does not extend to copyrighted information or material. The following statement must accompany the modified document: "Adapted from Air Command and Staff Research Report (number) entitled (title) by (author) ."

-- This notice must be included with any reproduced or adapted portions of this document.

REPORT NUMBER 87-2645

TITLE TECHNOLOGY TRANSFER--ITS IMPLICATIONS FOR DOD

AUTHOR(S) MAJOR TEDDY N. WANG

FACULTY ADVISOR LT COL ANTHONY A. MORRIS, ACSC/3824 STUS/CC

SPONSOR COL CALVIN R. JOHNSON, AWC/NP

Submitted to the faculty in partial fulfillment of
requirements for graduation.

AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY
MAXWELL AFB, AL 36112

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT **STATEMENT "A"** **Approved for public release;** **Distribution is unlimited.**
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) 87-2645	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION ACSC/EDCC 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State and ZIP Code) Maxwell AFB AL 36112-5542	7b. ADDRESS (City, State and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State and ZIP Code)	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO
11. TITLE (Include Security Classification) TECHNOLOGY TRANSFER--ITS IMPLICATIONS	
12. PERSONAL AUTHOR(S) Wang, Teddy N., Major, USAF	
13a. TYPE OF REPORT 13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Yr., Mo., Day) 1987 APRIL 15. PAGE COUNT 45
16. SUPPLEMENTARY NOTATION ITEM 11: FOR DOD	
17. COSATI CODES FIELD / GROUP / SUB GR	18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

This paper addresses the transfer of Western technology to the Soviet Union. By understanding the Soviets' efforts, organization, and methods to acquire Western technology, the reader can appreciate the significance of the technology transfer problem--especially to the military. The paper will also address current US controls to counter the exit of technology and concludes with recommendations that could further stem the flow of Western technology to the Soviet Union.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☒ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL ACSC/EDCC Maxwell AFB AL 36112-5542	22b. TELEPHONE NUMBER (Include Area Code) (205) 293-2483 22c. OFFICE SYMBOL

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

PREFACE

Many stories have been told about the Soviet propensity to copy Western weapon designs to satisfy their own military requirements. I have heard one where a battle-scarred B-29, forced to land in Soviet territory, was captured by the Soviets during the latter part of WW II. The aircraft was never returned to the United States. Instead, it was meticulously replicated--complete with bullet holes! Although the accuracy of the story is suspect, the Soviets did produce bombers after WW II based on the B-29 design.

Forty years later, the Soviet Union is testing its version of the US Space Shuttle. At first glance, the Soviet shuttle looks remarkably similar to ours. Upon closer inspection, the two shuttles appear almost identical! Could it be just coincidence?

I wanted to explore the possibility that the Soviets are copying valuable hardware developed in the United States. My initial search for Soviet thievery led me to believe that nowhere is this problem more prominent than in the area of high technology. Realizing that the United States is very dependent on technology, especially in its weapon systems, I chose to look into the problem of transferring high technology to the Soviet Union. My concern was finding enough information to support the assertion that the Soviet Union is stealing US technology.

As it turns out, ample evidence is available from unclassified sources to conclude that the United States has a problem stopping the loss of technology to the Soviet Union. I intend to examine the problem from a broad perspective and use several examples to illustrate the points being made. I will then give seven specific recommendations that can help alleviate the problem.

This paper and its recommendations are intended to be part of a briefing package used by the National Security Briefing Team based at Maxwell AFB, Alabama. The recommendations are themselves topics for further research to answer "how" these recommendations can best be implemented.

CONTINUED

ACKNOWLEDGEMENTS

Several individuals made the completion of this paper possible. My sincere thanks go to Lt Col Anthony Morris, Air Command and Staff College advisor, for his guidance and recommendations. I also want to thank Maj Thomas "Dutch" Miller, Faculty Instructor, for his assistance in editing and structuring major portions of the paper. Finally, my deep appreciation goes to Col Calvin Johnson, AWC/NP, for his advice and sponsorship of this project.

ABOUT THE AUTHOR

Major Teddy N. Wang graduated with high distinction from Arizona State University in 1971 with a bachelor's degree in mathematics. A distinguished graduate of a 4-year AFROTC program, Major Wang continued his education in mathematics and received his master of science degree in 1972. He was also selected in Who's Who Among Students in American Universities and Colleges that year.

Entering active duty in 1973, he served as an expert-level Space Surveillance Officer at Mill Valley AFS, Ca. In 1974, he wa stationed at Ko Kha AFS, Thailand, and was the first officer to qualify in all three operations positions at that spacetrack site. Returning to the CONUS in 1975, he was assigned as an Astrodynamics Analyst and part of the 427M NORAD computer upgrade team at Colorado Springs. He then served three years at the Air Force Academy Preparatory School as a math instructor and in 1981, taught at the Air Force Academy Department of Mathematical Sciences as Senior Course Director and Assistant Professor. In 1983, he was a member of an Air Force team at Johnson Space Center, Houston, Texas, serving as a NASA Flight Controller responsible for the attitude and pointing of the Space Shuttle Vehicle. As such, he supported the first (Solar Max) repair mission in space, the first retrieval of satellites (PALAPA and WESTAR) in space and their return to Earth for refurbishment and relaunching, as well as the first dedicated Department of Defense Space Shuttle mission. He was selected in 1985 as the Deputy Director, Development and Operations prior to being assigned as a member of the Air Command and Staff College class of 1987.

TABLE OF CONTENTS

CONTINUED

EXECUTIVE SUMMARY

Part of our College mission is distribution of the students' problem solving products to DoD sponsors and other interested agencies to enhance insight into contemporary, defense related issues. While the College has accepted this product as meeting academic requirements for graduation, the views and opinions expressed or implied are solely those of the author and should not be construed as carrying official sanction.

"insights into tomorrow"

REPORT NUMBER 87-2645

AUTHOR(S) MAJOR TEDDY N. WANG

TITLE TECHNOLOGY TRANSFER--ITS IMPLICATIONS FOR DOD

I. Problem: An increasing number of Soviet weapon systems have benefitted from technology developed in the West. This trend is disturbing because the United States cannot afford to contribute to Soviet weapons development, let alone help the Soviets acquire weapons that are ultimately deployed against the United States and its allies. Stopping this trend requires an understanding of the problem and developing solutions that can reverse the tide.

II. Objectives: To investigate the transfer of Western technology to the Soviet Union and to make recommendations that will stop the Soviets from further acquisitions.

III. Discussion of Analysis: The assertion that the Soviets are stealing technology from the United States to be used in their own weapons raises the following questions: (1) Are the Soviets randomly coming across "interesting" technical findings for integration into their weapon systems or is there a coordinated effort to acquire Western technology? (2) If there is a conscious effort to acquire Western technology, how successful have the Soviets been? (3) Have the United States and its Western allies been making efforts to curb Soviet efforts? If they have,

CONTINUED

why haven't they been more successful? (4) How can the United States improve current methods used to fight technology transfer to the Soviet Union? Answers to these questions were researched using the most recent resources available on technology transfer.

IV. Findings: The problem of technology transfer to the Soviet Union is real. Acquiring advanced Western technology is an area the Soviets take very seriously. They have developed a bureaucracy to direct and coordinate their national resources to acquire selected technology from the West. The Soviets use a variety of means to acquire the know-how and hardware necessary for developing similar technology themselves. Even after the Soviets have the technology to develop a specific capability, they still attempt to obtain information on Western technology either to improve their systems or to develop countermeasures against Western weapons.

US efforts to stop the Soviets from acquiring Western technology have been overshadowed in the 1970s by détente and the desire to trade competively in the world market. Agencies tasked to enforce export control laws became woefully understaffed and underfunded. As a result, militarily significant technology along with dual-use technology were lost to the East. US allies were also distrustful of US attempts to impose trade restrictions on some technology. The allies' suspicions were exacerbated by perceived inconsistencies in US foreign policy. Several members of COCOM (Coordinating Committee for Multilateral Export Controls) and neutral nations had their own self-serving interests in mind by selling militarily significant technology to the Soviet bloc. If the United States did not, in turn, sell similar items to the Soviets, US competitiveness in the high-tech market would be diminished.

V. Conclusions: The Soviets are still deploying new weapon systems containing advanced technologies acquired from the West. Not all were obtained in the 1970s. Although the Reagan Administration has slowed the flow of technology to the Soviet bloc by launching a significant program to counter the Soviets' efforts, losses still occur. The Soviets have hardened their resolve by recruiting technology-specialized KGB agents in addition to East-

CONTINUED

[illegible] agents to covertly acquire desired technology from the West. Moreover, a vast amount of sensitive information can be acquired through open sources in the United States by the Soviets--just for the asking. Although progress to stop technology transfer to the Soviets have been made, there is more that can be done.

VI. Recommendations: The United States needs to create a policy-making level organization to direct and coordinate US efforts to stop technology transfer to the Soviet Union. A cabinet- or National Security Council-level organization is necessary because [illegible] will impact both foreign and domestic policies. More effort needs to be made in working with COCOM and technology-producing nations to cooperate in denying militarily significant technology to the Soviet Union. Penalties for unauthorized sale or diversion of sensitive technology need to be made severe for both domestic and foreign violators. To improve domestic security, a comprehensive review of security clearance programs for defense contractors also needs to be made. Everyone working on sensitive projects needs to have his clearance periodically updated. These are some of the more significant steps that can be taken to counter technology transfer.

Chapter One

INTRODUCTION

Western technology is extremely important to the defense of the Free World. It is often used as an equalizer or force multiplier--compensating for the West's numerical shortfall. The United States relies on its qualitative edge in technology and maintains a numerically inferior military force that is still credible enough to deter a Soviet attack. According to former Secretary of Defense Harold Brown,

> There are alternatives to this reliance on technology: doubling the number of US personnel under arms to approach Soviet levels, increasing defense procurement budgets by 50 percent over what they would otherwise be to compete with the Soviets in quantities of equipment, and substituting purchase of production by allies for much of the current US production of military equipment (4:243).

In almost all weapon categories, the Soviet Union maintains a quantitative edge (see Appendix).

This paper addresses the problem of technology transfer to the Soviet Union. Chapter One includes this overview, followed by the definition of "technology" and other key terms so that the reader can share a common ground of understanding. A brief background on technology transfer and an assessment of the seriousness of the problem will then be discussed. (The Soviets are interested in the West's technological progress because they regard Western system characteristics as a yardstick against which their technical capabilities are judged (33:107). They spend the equivalent of $1.4 billion per year to underwrite their technology acquisition effort (31:108).) In fact, the Soviets have developed an entire bureaucracy to deal with the acquisition and evaluation of high technology. This chapter concludes by examining the organization and composition of that bureaucracy.

The bureaucracy directs the use of several methods to gather information on technology. The methods are not only integrated, but are part of a massive centrally-controlled campaign to obtain needed products and technical knowledge through legal and illegal means (31:108). Chapter Two discusses the methods used in the past and gives an assessment on the successes of these methods.

The Department of Defense (DOD) plays the key role in the government-wide domestic and international effort to safeguard US technology lead (31:151). Other government agencies, however, also cooperate to deny Soviet acquisitions. Chapter Three discusses the roles of the DOD and other agencies in countering the "hemorrhage" of critical technologies to the Soviet Union (28:54). Also discussed are the key laws that enable the agencies to control the loss of technology. The United States cannot win the war against technology transfer alone, however, but needs the cooperation of COCOM (Coordinating Committee for Multilateral Export Controls). Many COCOM members possess the same technology found in the United States. The role of this committee will also be discussed in this chapter.

Chapter Four explores the difficulties of enforcing control laws by raising some fundamental issues of tough enforcement. At what point is national security more important than the embargo of items that might be militarily significant? Trade not only promotes domestic economic growth, but is also considered in foreign policy. Another issue is freedom of information. Americans cherish their open society. Unnecessary restriction of information is not only undesirable, but can have a detrimental effect on healthy exchanges of information critical to creativity and technological growth. Another vexing problem comes from dual-use technology. What should the United States do about commercial technology that was never intended for military application, but can be modified for military use? These are challenging issues and they will be discussed in this chapter.

Chapter Five concludes this paper by stating the significant findings made in researching the problem of technology transfer to the Soviet Union. Also included are the recommendations that if implemented, will reduce the transfer of technology to nations outside the West, principally the Soviet Union, while protecting the fundamental principles of Western democracy.

DEFINITION OF TERMS

Technology. Technology is the know-how to specify, design, build, maintain, and use a product (7:117). It is, in part, experience-based know-how which transforms science into products and processes. Further, it is a collection of scientific principles, engineering procedures, and practices (13:49). Technology can consist of any information, equipment, or process which contributes to turning a concept into a useful product (18:44).

Contrast the above definition with Webster's Dictionary which defines technology as a technical language, a technical method of achieving a practical purpose, and the totality of the means employed to provide objects necessary for human sustenance and comfort (12:1197).

For the purposes of this paper, the reader should use the first definition. Note that technology includes knowledge, as well as sophisticated machinery.

Technology Transfer. Although some consider technology transfer as the free exchange of ideas (6:62), this paper will use technology transfer as the conveyance of technology from the West to the East--especially, the Soviet Union.

Technology Diversion. The transfer of technology to an unauthorized destination by an intermediary without the explicit approval of the United States. The intermediary may or may not be a legitimate recipient of the technology.

Dual-Use Technology. Civilian technology with potential military applications (4:27).

Espionage. The covert collection of information and/or equipment. Methods of collection include, but are not limited to bribery, extortion, and exploitation of susceptible individuals.

PROBLEM BACKGROUND

Technology acquisition from the West is not a new problem.

> Soviet attempts to acquire and benefit from advanced Western technology date back to at least the 1930s and Stalin's industrialization program, the program being motivated, in part, by Stalin's intepretation of Russian history and the damaging consequences of "falling behind" (8:169).

The Soviet Union wants to acquire Western technology for several reasons. After WW II, the acquisitions were used primarily as a stop-gap measure until their own growing research and development (R&D) programs could pick up (13:42). Even after these programs matured, however, Soviet collection efforts did not cease. It was evident that foreign technology acquisitions improved the quality and effectiveness of Soviet weapons (31:151), allowed them to incorporate second-generation Western military systems, enabled the Soviets to reduce their own R&D risks, and also allowed them to develop prospective countermeasures even while developing the original weapon systems (32:110).

PROBLEM SIGNIFICANCE

The transfer of US technology to the Soviet Union seriously undermines the qualitative US lead which contributes to US deterrence. The Soviets have successfully cut the lead time from 10-12 years in the 1960s, to 3-5 years (or less) at present (13:51).

For example, one of the key components to "ruggedized" military computers in advanced weapons is bubble memory. Bubble memory stores more information than standard computer chips and does not need power to retain its continuous memory. These are characteristics that can be incorporated into weapons--making them smaller and more reliable. Unfortunately, bubble memory technology (discovered by a Hungarian on US-funded grant) was transferred to the Soviet Union, advancing similar Soviet technology by at least 10 years (33:110).

Acquisition of Western technology saves the Soviets not only time, but also money. A DOD pilot study showed that had export license applications for a significant number of illegal diversions in 1983-84 been approved, the Soviets would have saved between $6.6 and $13.3 billion in primary military research costs during the 1990s and beyond (32:21). The Soviets would also have saved hundred of millions, if not billions of dollars by utilizing proven US designs to field counterpart systems (32:21).

The Soviets also satisfy their defense requirements through "reverse engineering" (2:16), imitating, and integrating Western technology. For example, the MiG-29 FULCRUM all-weather, air superiority fighter-interceptor is effective against US cruise missiles because of its Western-developed look-down/shoot-down radar technology (32:79). The An-72 COALER short-takeoff-and-landing aircraft is a copy of the Boeing YC-14, an undeveloped US aircraft (33:110). The Soviet Il-76 CANDID bears striking structural and performance similarities to the Lockheed C-141, one of which was carefully inspected by the Soviets during a Paris Air Show (33:110). There are many more examples.

Soviet Bureaucracy

To further underscore the significance of the technology transfer problem, it is helpful to note the Soviet Union's total effort in obtaining advanced Western technology by examining a special Soviet bureaucracy. This bureaucracy not only identifies technology requirements, but also directs acquisition efforts. Some of the more significant requirements will be discussed along with what the Soviets think are the most important technologies to acquire. Knowing this will give the United States a gauge with which to measure the success of Soviet efforts in acquiring the technologies they need. As will be pointed out later, the Soviets' carefully executed program through both legal and illegal means (32:19) have been immensely successful.

There are six key organizations: KGB (Soviet Intelligence) (31:125), VPK (Military-Industrial Commission) (31:108), GKNT (State Committee for Science and Technology) (6:238), GRU (Chief Intelligence Directorate) (8:10), Ministry of Foreign Trade, and the State Committee for External Economics Relations.

The main coordinating body is the VPK of the USSR Council of Ministers operating under the guidance of the Party Central Committee. This commission tasks the KGB (Directorate T of the First Principal Directorate) (7:68) and the GRU to covertly collect militarily useful technology. GKNT is also intimately involved in the coordination of basic scientific research under Central Committee authority and helps determine which scientific need can best be met through intelligence collection (6:238). The Ministry of Foreign Trade administers a trade diversion program to obtain a significant number of manufacturing and supporting equipment for direct use on Soviet military-industrial production lines (31:108). Surprisingly, these covert activites represent a small part of the Soviets' total effort. By and large, the Soviets primarily work openly and legally (7:68).

Using the organizational structure outlined above, the Soviets have been very successful in acquiring foreign technology. For example, the VPK has directed over 3,500 requirements each year during the late 1970s and early 1980s. About one-third of that number were satisfied annually (31:108).

Soviet Requirements, and Soviet Priorities

The Soviets can satisfy some modern military requirements much more efficiently by technological acquisitions from Western state-of-the-art designs than they could ever hope to achieve themselves due to lower technology levels. Military needs for AWACS-like aircraft, floating drydocks, antisubmarine weaponry, armor, antitank system, aerospace, shipbuilding, heavy vehicle, metallurgy, machine building, telecommunications, lasers, jet engine fabrication, radar, guidance and navigation, and precision manufacturing (13:42-51) can all benefit from technological infusions relevant to computers, microelectronics, and advanced machinery. It's no surprise that primary Soviet targets of Western technology include electronics, computers, manufacturing technologies, structural materials (33:105), and robotics (31:108). Soviet intelligence collections in the past 15 years have also emphasized rocket propulsion, missile defense, and "smart" bombs (6:67). The next chapter discusses how the Soviets attempt to acquire these technologies.

Chapter Two

ACQUISITION METHODS AND SUCCESSES

The Soviets employ six basic methods in gathering Western technology: espionage, open sources, student exchanges, marketing/manufacturing companies, bilateral agreements, and business intermediaries (20:17). Using these methods, the Soviets were able to acquire 6,000 to 10,000 pieces of hardware and 100,000 documents annually. An average of more than 5,000 military research projects benefit each year (25:2). Although these methods are not all illegal, the Soviets have been increasingly forced to acquire technology through covert means because the US Government is tightening export control laws and procedures (32:19-20). One such means is espionage.

ESPIONAGE

The Soviets have placed major emphasis on espionage, creating a network of 20,000 (Soviet and Eastern bloc) agents available to steal Western technology (20:15). Most of these agents work for the KGB and GRU. Together they are tasked to acquire about 70 percent of the technology requirements (15:16). The KGB even has a special division known as Line X whose sole purpose is to obtain high-technology, data, and hardware (19:2). This is a special breed of spies who are very cultured, socialize easily at cocktail parties, dress well, have good language skills, and appear to be quite charming people. Gennadiy Fedorovich Zakharov is believed to be 1 of 300 Line X agents worldwide (19:2).

Another method the Soviets use successfully is the employment of Eastern bloc surrogates. East European agents are particularly effective because (1) they have a better image in the West than their Russian counterparts thus operating more freely, and (2) the Soviets ensure that there is a redundant channel available to acquire Western technology (28:54). In fact, through a Polish agent, the Soviets were able to acquire the know-how for the following radar systems: B-1 and Stealth quiet-type, F-15 look-down/shoot-down, Phoenix air-to-air, all-weather tank, shipboard surveillance, Patriot and HAWK surface-to-air, and NATO air defense (28:56-60). The price paid over a 3-year period was $110,000. The look-down/shoot-down fire control radar documentation alone allowed the Soviets to incorporate the system into the Su-27 and MiG-29 much earlier and cheaper by saving five years of

development time, $55 million research costs, and 1000 man-years of scientific research effort (25:2).

Open Sources

About 30 percent of Soviet technology requirements can be met by legal open sources (15:16): newspapers, magazines, trade and technical journals, government and contractor reports, public meetings, and hearings. Others estimate the percentage to be much higher. According to Jeffrey Richelson, an expert on Soviet intelligence, the Soviet Union spends the major portion of its intelligence and budgets on clandestine operations, but the vast majority (up to 90 percent) of the information employed in intelligence analysis is obtained from open sources (8:119). Another expert says, "without question, the most widely used technology transfer mechanism is the open literature" (7:125).

Unclassified information can easily be obtained. The best intelligence is derived from multiple independent sources, which can lend credence or substance to otherwise sketchy information, resulting in a total picture of significant value. The Soviets can take advantage of the open US environment that is the most "lenient" of all the Western countries--lacking even the Official Secrets Act of the United Kingdom (8:122). Soviet agents are able to obtain tremendous insight into developing weapon systems just by attending Congressional hearings. The 1983 House Appropriations Committee hearings alone produced nine volumes, with 600-1,000 pages per volume, containing present and projected capabilities, vulnerabilities, and development schedules of the Ground Wave Emergency Network, ASATs, laser experiements, as well as space-based early warning, nuclear monitoring, and strategic defense systems (7:130-131). The Strategic Air Command identified 21 other open sources as potential references on military affairs: National Technical Information Service documents, Defense Documentation Center unclassified documents, Aviation Week and Space Technology, Jane's Fighting Aircraft, Flight Operations, Military Affairs, Military and Space Daily Newsletter, Military Electronics/Countermeasures, The Infra-red Handbook, Aerospace Daily, Air Force Times, Combat Crew, Airman, Defense Management Journal, Commerce Business Daily, Armed Forces Communications and Electronics Association (sic), Electronics News, Electronics Warfare Markets, USA, Defense Electronics, Notices to Mariners/Airmen, and, various base and community newsletters (8:127-128).

Soviets find conferences invaluable. According to their own sources, millions of rubles (about 100 man-years of effort) were saved in long-range military research by using information obtained at seven professional conferences in the late 1970s and early 1980s (25:4). They seek every opportunity to exploit the openness of Western society--especially the scientific community.

STUDENT EXCHANGES

The Soviets also collect information on technology from US/USSR student exchange programs which have existed since 1950. The détente era encouraged these programs and in May 1972, United States and the Soviet Union signed an "Agreement in Cooperation in the Field of Science and Technology" (8:172-173). The Graduate Student/Young Faculty Exchange Program sponsored most of the Soviets involved in scientific and technological work and according to US intelligence assessments, at least three-fourths of the Soviet students are in the S&T (Science and Technology) fields (28:54). One such student, S. A. Gubin, was taught by a US Navy consultant on fuel air munitions. After his return to the Soviet Union, there was a marked increase in Soviet development and testing of these advanced technology weapons (28:54).

MARKETING AND MANUFACTURING COMPANIES

The Soviets also use their resources to invest in the formation of marketing and manufacturing companies "to buy high technology and munitions for illicit export to the Soviet Union and to serve as havens for spies...The (sic) tangled web of ownership of many US corporations obscured the identity of their true owners" (20:17). These companies are known as "bogus" or "fronts" used to evade the Export Administration Act of 1979. According to the CIA, there are over 300 companies overseas and about 20 in the United States engaged in diversionary schemes (8:172,175). According to the Director of Central Intelligence, William J. Casey, the 300 companies exist in over 30 countries, however, most are in West Germany (28:53). The existence of the companies is described as a network of businessmen who sell banned high technology equipment that cannot be easily acquired by other means (19:2).

Three examples illustrate how the Soviets use "front" companies to obtain critical hardware. In 1979, I. I. Industries in Sunnyvale, California, was convicted of shipping semiconductor processing equipment to the Soviets in 1975 and 1976 without an export license. The company simply mislabeled the equipment as goods that did not require a validated export license (3:88). Another example involved a Western middleman who established front companies in Yugoslavia, Switzerland, and West Germany (since those countries are not on the restricted list) to buy embargoed photoelectric repeaters from the David Mann Company (a US company) (8:176). Obviously, there was a breakdown in US intelligence because the United States did not anticipate the Soviets' need for the repeaters. In a more recent case, a husband/wife team (Walter J. and Frances A. Spawr) was caught shipping 50 laser mirrors to West Germany and Switzerland (6:352). Unfortunately, some of the mirrors got through and are now undergoing tests for use in Soviet killer satellites (3:88).

BILATERAL AGREEMENTS

The Soviets also seek to acquire information beneficial to both their long- and short-term research and development programs through bilateral agreements with Western nations. This method allows Soviet experts the opportunity to gain direct exposure to the best Western minds through bilateral agreements with the United States. Joint space ventures like the Apollo-Soyus Test Project in 1975 were beneficial to the Soviets especially in rendezvous and docking techniques. Soviet and East European scientists and engineers participating in academic, commercial, and official science and technology exchanges end up collecting information on know-how, equipment, and computer data bases (3:97). USSR Academy of Sciences and several of its institutes follow Western S&T, even tapping into Western data bases through a growing number of transnational computerized networks dedicated to S&T collection and dissemination (32:20). This is a real concern and the Pentagon is seeking ways to limit Soviet access to the data bases.

BUSINESS INTERMEDIARIES

One of the most successful and sophisticated methods the Soviets use to transfer technology is through a "third party" or "business intermediary." This is also known as trade diversion. The recipient or end-user of defense-sensitive equipment agrees that the product will not be reshipped or used for military purposes without explicit approval from the United States. In October 1984, the United States was fortunate to stop a Soviet attempt to divert a photomicrodensitometer from West Germany to East Germany. The Soviets had failed twice to obtain the equipment legally from the United States. The United States was able to detain the militarily useful equipment (needed for streak camera photography) at the East German border as it was bound for the Lebedev Institute in Moscow (31:20). In another example, the United States was less fortunate and did not stop the diversion of $5-7 million highly sensitive electronic parts for a computer-aided design workstation. The equipment was shipped by Tektronix, Inc., of Beaverton, Oregon to a cosignee in Cologne, W. Germany, where it was forwarded to Vienna (a well-known holding port for trans-shipment into the Soviet bloc). From Vienna, the equipment was shipped to an East European state, believed by many investigators to be Bulgaria (17:55). This problem is serious--as illustrated by the fact that in 1984, German and Swedish officials seized approximately 50 tons of advanced US computers and related equipment after being diverted through about half-dozen Western countries (32:108). There have even been cases where "legitimate" third party users either conspired to divert technology or simply looked the other way. This happened in Austria, where the problem was so bad in 1982, the United States threatened sanctions in retaliation (8:176).

Chapter Three

CONTROLS

When virtually all of the Soviets' 5,000 ongoing military research projects benefitted from Western technology (31:108), the adequacy of Western controls must be questioned. This chapter examines the agencies in the US government tasked to prevent technology transfers threatening US national security and an international committee organized to protect Western economic and security interests. It also discusses two major US laws specifically written to limit the export of Western technology.

DEPARTMENTS AND AGENCIES

Although there are over 40 agencies taking part in controlling technology transfers (13:50), 7 are key players: Department of Commerce, Department of Defense, Department of State, US Customs Service, Federal Bureau of Investigation, Central Intelligence Agency, and the US Attorney General.

Department of Commerce

The Commerce Department has the overall responsibility for stopping the transfer of technology because export control is part of its function (20:11). In fact, The Secretary of Commerce is given the lead role in the licensing of exports, the denial of licenses, and the administration of the Export Administration Act (EAA) (1:15). The EAA is a federal statute that limits the flow of technology from West to East (13:46), and is administered by the Department's Office of Export Administration (2:122). Basically, certain commodities may be controlled for national security and foreign policy purposes. The EAA is continuously reviewed and amended by Congress and the 1985 version includes the foreign availability element (30:30), necessary for granting export licenses on commodities already available overseas.

The Commerce Department is also active in controlling illegal exports in many other areas. Some of their responsibilities include inspecting cargo, identifying and investigating violations, administrating civil penalties, and forwarding criminal cases to the Justice Department for prosecution (2:102). Another traditional task assigned to Commerce is postshipment verification (2:113), where goods shipped overseas are checked at

destination ports. Commerce also administers the reexport of US goods through the distribution license system (23:25).

Prior to the Reagan Administration, the Commerce Department was not effective in carrying out its tasks and had been severely criticized for its poor record against illegal transfers. According to former Acting Director of the Office of Export Administration, Lawrence J. Brady, "controls could not be administered by the Commerce Department because it did not have the attention and resources it needed" (2:98). The Reagan Administration, the General Accounting Office, and Congress scrutinized the Commerce Department and found the Compliance Division (controlled enforcement office) deficient. It was poorly equipped, understaffed, had inadequate intelligence, and sometimes manned with undertrained and unqualified investigators (2:104). Moreover, it had no overall strategy to stop the exodus of technology (2:101).

To correct the inadequacies of the Compliance Division, the Office of Export Enforcement was established in its place (8:100). The office will receive a budget increase from roughly $1 million in 1982 to $10 million in 1987 (30:30). The staff was also increased from approximately 25 in the spring of 1982 to 164 in 1986. Additionally, six field offices were added in New York during FY 1986 (30:30). A second regulatory enforcement program known as the Office of Antiboycott Compliance was also established. To improve the effectiveness of the Commerce Department even further, the Foreign Availability Assessments Division of the Office of Export Administration was formed in 1984. It developed and maintained a data base of foreign high technology availability, especially in the Soviet Union and the People's Republic of China. This division will influence export decisions on US high technology (8:100). The Commerce Department is also increasing its intelligence operations in technology transfer. Information sought includes the party interested in acquiring such technology, the attempts to provide the technology, and its accessibility, especially through dual-use technology (8:98-99). These steps will improve the Commerce Department's ability to enforce export controls, but more needs to be done.

The Commerce Department is ironically contributing to technology transfer through its National Technical Information Service. Seventy-five percent of its publications contain Department of Defense, Department of Energy, and the National Aeronautics and Space Administration information (13:44). These reports are sensitive, but readily available to the Soviet Union. Another area of concern is objectivity.

The Commerce Department must deal with potential conflicts of interest. Asking Commerce to restrict technology trade is akin to "leaving the fox to watch the chicken coop." Theodore Thau, former Executive Secretary of the Export Control Review Board commented on the Department's poor enforcement record, noting

that Commerce has traditionally been interested in promoting exports, not in stopping them (2:255).

Department of Defense

The Reagan Administration is committed to stopping the illegal transfer of technology. In addition to giving Commerce more resources needed for effective export control, the Administration is also giving the Department of Defense a greater role (14:8). The DOD now shares a task once assigned exclusively to the Commerce Department--reviewing export license applications.

Several things led to this change. First, the Defense Department was genuinely alarmed at Soviet efforts to acquire Western technology. Secretary of Defense Casper Weinberger was convinced the Russians were "looting the United States, legally and illegally" (20:11). Second, legislation was written to support DOD's efforts to play a more active role in export control. Richard N. Perle, Assistant Secretary of Defense for International Security Policy had written key legislative provisions (while a staff assistant to Senator Jackson) expanding the authority of the Secretay of Defense (14:9). The Secretary of Defense is now authorized to assess whether exports of goods and technology to certain restricted countries would make a significant contribution to their military potential, and he can recommend to the President whether export licenses should be granted or denied (1:15). Third, Commerce had not been effective in the past. The consequences of Commerce's poor performance in controlling technology transfer in the 1970s are still being felt in the 1980s. In 1972, The United States sold to the Soviet Union technology needed to develop the Kama River truck factory (2:94-95). As a result, the Soviets have the largest truck factory in the world (3:132) producing military-specification trucks to support the Afghanistan invasion (3:94-95). Also in 1972, the United States sold to the Soviet Union specialized machines, made by the Bryant Chucking Grinder Company of Springfield, Vermont, that will grind high precision ball bearings used in Soviet MIRV ICBM guidance systems, jet engines, high-speed aircraft, and complex steerable space-antennas (2:260-264). The wisdom of the sale was again debated by Congress in 1983 (2:264).

Consequently, President Reagan overrode Commerce and lobbyist objections, and in January 1985 directed the Defense Department to review militarily applicable technology export license applications (14:9). The Defense Technology Security Administration (DTSA) was created and tasked to review export applications sent from Commerce's Office of Export Administration. The DTSA has 45 days to give its assessment (27:13).

Although Perle claims that "massive leaks" of Western technology have been stopped (25:5), the problem is far from solved. The DOD cannot prevent control breakdowns by itself, but often

shares the blame when breakdowns occur. Dr Stephen D. Bryen, the Deputy Assistant Secretary of Defense for International Economics, Trade and Security Policy, is the Pentagon's top policy maker in charge of curbing technology transfer to the Soviet bloc (19:2). He has been given a clearcut mandate and money for halting the flow of American technology eastward to the brain trust and military market of the Soviet Union (20:11). Called before the Senate Banking Committee, he had to explain how eight containers of US strategic goods and a VAX 11-782 computer system were illegally diverted to the Soviet Union in 1983 (23:25). As it turned out, William T. Archey, Commerce Acting Assistant Secretary for Trade Administration conceded his department's failure (23:24). He blamed the failure in stopping the diversion to "a three-year sequence of intelligence, analysis, and communication breakdowns inside Commerce" (23:24).

Defense faced other problems. Its increasingly active role was not unanimously embraced. The Pentagon's participation in stopping technology transfer eventually led to sources overseas and negotiations with foreign governments. This unavoidable progression of events transgressed into traditionally enshrined territory belonging to the State Department. It's no wonder that the State Department objected to the Pentagon's "encroachment" (2:131) and even accused the DOD of "making a power grab" (2:130-131).

Department of State

As suggested earlier, the State Department is the US government's interface with foreign governments. In the past, it has cooperated with the Commerce Department and assisted in overseas enforcement of export controls (2:102). Members of the State Department have worked with Commerce by providing help from US embassy officials for postshipment verification. This was not a primary job for State officials who found the task of postshipment verification frustrating. "Many foreign service officers... had difficulty in knowing what they were looking for--or at" (2:113). Additionally, the Office of East-West Trade leads the US delegation for COCOM (Coordinating Committee for Multilateral Export Control) and headed the conference in January 1982 (2:128). The State Department also plays an important part in strategy formulation for controlling technology transfer.

State is a key member of interagency groups responsible for the coordination of export controls. Foreign policy considerations are valid reasons for imposing controls on goods and technology (2:137-138). Actions that could adversely affect US export performance or are inconsistent with overall US foreign policy need to be considered and articulated prior to imposing controls on certain commodities.

US Customs Service

The "agency without a mission" was how one source described the Customs Service during 1980-1981 (2:88). Its role had been to respond to requests from Commerce's Office of Export Administration to undertake searches, seize cargo, and make arrests. Things changed in October 1981 after the Customs Service mounted Operation Exodus--a counteroffensive against high technology smuggling (2:88). The massive cargo inspection program netted $20.5 million in illicit exports during the first six months with the DOD financing the $28 million operation and Commerce determining whether licenses were in order. According to US Customs Special Agent Kenneth Ingleby, one-third of the agents and resources from his San Diego office was devoted to Operation Exodus (21:11). Between October 1981 and August 1982, $50 million worth of goods headed for suspicious destinations from nearly every major airport were seized (20:14). Before Operation Exodus, the Customs Service had only four inspectors whose job it was to ferret out high technology items not authorized for export--four for all of the airports, ports, and other gateway out of the United States (20:11). Afterwards, Customs began training hundreds of agents in the art of detecting technology contraband. Traditionally, US Customs Service had foreign investigation responsibilies in smuggling and in export investigations (2:112). But, the Commerce Department still had primary responsiblities for technology transfer enforcement (2:102). Both the Treasury and Justice Department, however, are in favor of Customs taking over the enforcement responsibilities (2:103).

Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) participates primarily in criminal law enforcement and domestic counterintelligence roles (2:102). Additionally, President Reagan signed Executive Order 12333 which allows the FBI to do the following:

> Conduct within the United States, when requested by the officials of the intelligence community designated by the President, activites undertaken to collect foreign intelligence or support foreign intelligence collection requirements of other agencies within the intelligence community (8:103-104).

Such activities include wiretappings and break-ins. The phones of an allied trade mission in San Francisco were even monitored (8:104) to preempt trade diversions.

Central Intelligence Agency

The Central Intelligence Agency provides information on violations abroad. It also devotes its expertise to technology transfer because intelligence is critical to the success of

countering illegal transfers. About 30 analysts are working full time to track high technology items that might be of value to American enemies (20:14). Dr Stephen D. Bryen declares, "there is a war on, the Pentagon wants other involved government agencies to know about it" (20:14). Dr Bryen is also generating a computer data base for records and profiles. Under the Reagan Administration, and Central Intelligence Director William Casey, the number of National Intelligence Estimates (NIEs) rose to 38 in 1981, and 60 in 1982. Among other assessments, the NIEs included estimates on Soviet dependence on Western technology and trade for its military buildup, and the impact and effectiveness of allied trade sanctions against the Soviets (9:245).

US Attorney General

The US Attorney General's office cooperates with other federal agencies and prosecutes criminal cases. In California, for example, the US Attorney General established a Critical Technologies Task Force, including Assistant US Attorneys, postal inspectors, and representatives from the Commerce Department, Customs, the FBI, and the Internal Revenue Service. The Task Force is setting up law enforcement coordination links with state and local police, as well as technolo businesses in the area. Because the Soviet Union is behind most of the industrial espionage, the intelligence community also works closely with the Task Force and is part of a national effort to stem the hemorrhage of critical technology to US adversaries (15:20).

LEGISLATION

Export Administration Act

The first attempts to control US exports occurred in 1940 (1:4) and have continuously evolved in response to changing world conditions and national interests. On 26 February 1949, Congress passed the Export Control Act designed "to deny the Soviets any trade that would contribute to either their military or econonmic potential" (1:4). The era of détente resulted in the Export Administration Act (EAA) of 1969, which lifted the ban on those products and technologies that would strengthen the Soviet Union's "economic potential" (1:5). This relaxation of export controls brought concerns to the Department of Defense, and the EAA was amended in 1977 to give the DOD more authority to review exports to any country. In 1979, a new EAA was passed and includes the following provisions: (1) minimize uncertainty in export control, (2) separate criteria and procedures of controls enacted for national security from those instituted for foreign policy reasons, (3) make the licensing process more efficient, (4) allow the exemption of validated (versus general) licenses if items are available elsewhere, (5) give the President total discretion in deciding to apply foreign policy controls, and (6)

charge the Secretary of Defense with primary responsibility for developing a Military Critical Technologies List (MCTL) (34:18-19).

The MCTL was first published in January 1980 and revised in November 1981 (34:37). Both lists were classified and the second was 800 pages long. The List was to be specific enough to guide validated licensing decisions, and to become part of the Commodity Control List (34:82). Representative Don Bonker (D-Wash.) noted that there are over 200,000 items on the List, including home personal computers, telephones and the wiring that goes into lightbulbs. Congress had envisioned the MCTL to consist of (1) an array of design and manufacturing know-how; (2) keystone manufacturing, inspection, and test equipment; and (3) goods accompanied by sophisticated operation, application, or maintenance know-how which could significantly advance another country's military system (34:82).

Battle Act

The Battle Act is also known as the Mutual Defense Assistance Control Act of 1951 (1:4). Among other things, it requires an embargo of strategic products and materials to any nation that threatened the security of the United States. This law also requires negotiations with other nations to obtain their cooperation in controlling exports to the USSR and Communist bloc countries. These negotiations are currently taking place with COCOM, the informal group concerned with both security and economic issues (1:5). For the most part, the provisions of this Act have been included in the Export Administration Act of 1979 (2:138) and is mentioned here for completeness.

COCOM

COCOM (Coordinating Committee for Multilateral Export Controls) was created in November 1949 for the purpose of coordinating its members' national controls over the export of strategic materials and technology to the communist world (11:148). This committee began operations on 1 January 1950 with 7 member nations and currently has a total of 15 members (22:21). These include all NATO nations (except Iceland) plus Japan (25:2). Nonmembers of the Paris-based COCOM include Switzerland, Sweden, New Zealand, and Australia (10:57-59). This fact is significant because nations like Switzerland can play the role of an arbiter while nations like Sweden have been a source of "leakage."

COCOM is obviously another key player in the success or failure of countering technology transfer. An agreement of what technology (commercial and military) should or should not be sold to the East must be unanimous (25:2). Agreement is not easy since for some COCOM members, trade with the Eastern Bloc forms a

significant part of their economy. For example, West Germany's trade with the communist countries amount to 6.2 percent of their total trade (3:22). Not surprisingly, West Germany is the single largest supplier of Western technology to the Soviet Union (2:23).

Chapter Four

FUNDAMENTAL ISSUES

Trade becomes an issue when restrictions are placed on goods having potential military significance because those goods are no longer accessible in the commercial market. Another issue is the restriction on information to the public, as guaranteed by the First Amendment, because its release could jeopardize national security. A third issue is related to the first. Should commercial products, available in electronic stores, be restricted from trading abroad because they can be modified for military use? This chapter will not resolve these issues. They are mentioned here to give the reader an appreciation of the complexities in dealing with export controls.

ECONOMICS VS SECURITY

Domestic

An article in the 19th Edition of Air War College Associate Programs chapter states the problem this way:

> US companies cannot even agree with each other on the extent that the Federal Government should participate in controlling offsets [countertrade]. If US interests cannot agree among themselves, can we realistically expect our allies to control offsets, particularly when a US company is competing with one of their own (13:55)?

Domestically, there are issues other than national security: employment, foreign trade, international political relations, and the economic growth and development of friendly countries (2:20). Additionally, there is a lack of consistent interpretation on militarily significant technology. Export license decisions have reflected judgments based not only on technical military assessments, but also on the political climate (34:82). Even Congress is undecided on what the export administration policy goals should be. Should the emphasis be primarily on US national security, diplomatic options, efficient/consistent licensing system, or trade promotion (34:87-88)?

While debate continues, some in industry are complaining that current US controls are stricter and more onerous than foreign

ones , and therefore are unfair impediments to American exporters (22:22). It is clear that national security is not the only concern. Theodore W. Wu, Deputy Assistant Secretary for Export Enforcement, suggests a balanced approach to strategic export control, and not create unnecessary export disincentives (30:30).

Foreign

The US goal is to convince its friends that selling or diverting militarily significant technology to the Soviet bloc is detrimental to Western security. Former Secretary of Defense Harold Brown suggested the following solution:

> The United States should put pressure on its allies to agree [on export controls], recognizing that its [US] leverage is limited.... But the United States has technology that its allies want, and this technology could be held back if the allies fail to agree to enforceable restraints on its retransfer to the Soviet bloc (7:31).

This seems like a simple plan, but there are many complex obstacles to overcome. First, there are several non-COCOM high technology-producing nations that are neutral. They do not participate in any trade restriction talks with the United States and could conceivably take the market away from COCOM members complying with export control agreements. Second, COCOM (similar to the US Commerce Department) is interested in both economic and security matters. Its members want to bolster their economy by promoting trade whenever possible, perhaps even at the expense of security; disagreements often result. Third, some COCOM members perceive the United States pursuing an inconsistent embargo policy. The United States often does appear to place self-interests first. Fourth, even if COCOM agrees on an embargo, there is little the organization could do if a member cheats. These difficulties need to be discussed separately.

Taking a look at the first obstacle, the Pentagon released a "grey list" of countries that might divert technology to the Soviet bloc. It includes the following countries: Austria, Finland, Hong Kong, India, Libya, Liechtenstein, Malaysia, Iran, Iraq, Singapore, Spain, South Africa, Sweden, Switzerland and Syria (26:45). Although not all are high technology-producing countries, negotiations are taking place with some to tighten their national controls and progress is being made. Spain, for example, is now a member of COCOM and others are bringing their high-tech regulations in line with US regulations.

The second obstacle is perhaps the most difficult for COCOM to overcome. What the United States sees as a military risk, COCOM often sees as an economic venture. Europeans have accused the United States of "high-tech protectionism" and have suggested

that US export control policy represents collusion between elements of the US government and major US exporters to defeat foreign commercial competitors (21:3). Former Executive Secretary of the Export Control Adminstration Review Board, Theodore L. Thau believes COCOM has always been a servant of business interests over security interests (2:126). Richard Perle shares this view saying that "[COCOM] is a regulatory institution with the regulees present.... The potential for self-deception is very large" (2:127). Unfortunately, the United States is not above scrutiny.

The United States has been accused of having self-serving and inconsistent trade and foreign policies. The British high-tech industry was unhappy when the United States relaxed trade restrictions with China, allowing the sale of equipment subject to COCOM controls (2:139). Questions were also raised about the US sale of Digital PDP 11 computers to Yugoslavia, and the heralded 1983 seizure of VAX 11/82 computers at the Dover docks in Sweden when the identical computing machines were already in Moscow hospitals (2:140). The Confederation of British Industry, representing the top twelve thousand UK companies claimed that the use of controls had negligible effects on Soviet policies and the main result of embargoes had been to alienate trading partners and allies (2:134). Another example of apparent inconsistency was for President Reagan to lift the grain embargo President Carter had imposed in response to Soviet invasion of Afghanistan, and then imposed oil and gas technology embargo because of martial law in Poland. President Reagan then also attempted to prevent foreign firms from exporting petroleum equipment technology to the USSR. France, United Kingdom, West Germany, and Italy defied the US orders (34:4-5).

As suggested earlier, COCOM is not based on a formal treaty and has no legal status (20:15); its members are legally free to ignore COCOM controls. Moreover, there are always intense domestic pressures within member nations to seek trade. For example, when President Carter disapproved the license for a $6.8 million Sperry computer system in 1978 destined to the Soviet Union, the French immediately jumped at the chance and offered the Soviets an even larger computer and "thumbed its nose at COCOM" (2:125-126). The British also ignored COCOM controls in the 1970s by selling Rolls Royce, Ltd. Spey supersonic military engines to the People's Republic of China (3:88). Rep. Jonathan B. Bingham, then Chairman of the House Subcommittee on International Trade, noted in a letter to President Reagan on 29 October 1981: "In my view, circumvention of US and multilateral export controls has contributed more to Soviet military capabilities than the technology approved for sale (3:88).

FREEDOM VS SECURITY

Freedom in the United States, ironically, can threaten the security of the United States. As pointed out in Chapter Two, the Soviets depend heavily on readily available unclassified sources in the United States for their information on technology. Using the Freedom of Information Act (FOIA) to obtain information for intelligence is an exclusive latter-day American phenomenon. Britain and the Commonwealth have their Official Secrets Acts. Even liberal Sweden prosecutes journalists for merely discussing the existence of a Swedish intelligence service (5:296). The FBI and CIA together spend over 400 man-years, every year, responding to FOIA requests (5:297). For the sake of US security, some have suggested that controls or restrictions be imposed on access to previously open sources.

Controlling freedom of information is an issue that goes to the heart of a free society where information is exchanged with few restraints. One reason given for this nation's technological successes has been the ability of its scientists, engineers, researchers, and managers to share their knowledge. Ideas are formulated and exchanged from many sources: symposiums, public media, and professional journals. These ideas are often researched and result in many benefits, including advanced technology. Any attempts to thwart an open atmosphere of learning and discussion have generally been oppposed. For example, officials at University of California at Berkeley were even against Pentagon efforts to limit Soviet bloc scholars and students access to the Cray X-MP, a supercomputer--the "crown jewels of US technology" (16:1).

Other critics have charged that the Administration's program of technology security undermines the economic and scientific progress essential to the long-term national security (38:4). Academicians claim it would be politically repugnant for the government to interfere with information exchanged in the realm of theory, basic research, and lab experimentation (3:15), because these are the fundamentals leading to new discoveries, not all affecting national security. Another controversial issue is controlling dual-use technology transfers.

DUAL-USE TECHNOLOGY

Dual-use technology falls in a grey area. While such goods are for civilian/commercial use, they may have significant military application. Examples of dual-use technology items include computers, fiber optics, jet engines, semiconductors, sensor and seismic technology, and telecommunications equipment (3:3). Minicomputers designed for routine lab work can be used to control nuclear weapons production; laser technology exported for manufacturing purposes can be modified to be exotic satellite-

killing weapons; computers for weather forecasting and air-traffic control can be programmed to direct missile launches; and special drill bit machinery for oil and gas exploration can be used to make armor piercing warheads (7:189). The Soviets have used drydocks, promised for civilian purposes, to repair Kiev-class aircraft carriers, nuclear powered ballistic missile submarines, and other warships (15:18).

It is government policy to restrain export of militarily significant goods without interfering any more than necessary with peaceful trade (3:16). The problem is that almost every militarily significant technology has peaceful uses. The House and the Senate are concerned that controls which are too strict will not weaken the Soviet's ability to obtain products, but will unnecessarily restrict US exports (13:46).

This is a difficult issue to resolve. A related issue is how to determine which dual-use technology to restrict. The problem becomes even more acute as high technology becomes more available worldwide. Export control talks with high technology-producing nations are a must.

Chapter Five

CONCLUSION

This chapter concludes this paper by giving the findings of the research project. Also included are the recommendations that if implemented, can solve the problem of technology transfer to the Soviet Union.

FINDINGS

The United States lost significant militarily sensitive technology to the Soviet Union since WW II through both legal and illegal means. The loss eroded the qualitative US lead in technology, gave the Soviets additional military capabilities, and also gave them the means to counter the latest US weapons. The Soviets used the acquired technology to develop accurate MIRV ICBMs for striking hardened targets, produce trucks for invading Afghanistan, deploy Il-71 and An-72 for strategic and theater airlift capability, and integrate the look-down/shoot-down radar system in their fighters for shooting down low-flying aircraft. They are also testing laser weapons using US-developed mirrors.

Efforts to counter the loss of technology have been partially successful. The Washington Times on 26 August 1986 reported that the United States has been able to inflict a major setback to Soviet high-tech espionage through increased efforts to ferret out elite KGB spies (19:2). The article also added that several Line X officers (see Chapter Two: Espionage) were among the 100 Soviet KGB spies arrested in or expelled from Western countries since 1981. At least one was traded for Anatoly Shcharansky (19:2). However, it is widely accepted that the Soviets will continue to emphasize clandestine activities focused primarily on the acquisition of scientific and technological data in the United States, Western Europe, and Japan (33:127). Soviet espionage efforts have netted them tremendous gains, and they will continue to use this profitable method to collect Western technology.

Soviet acquisition of technology through open sources will always be effective since the method is relatively cheap and because of American propensity towards various freedoms, academic and press being two of the most obvious. Totally effective control of information is impossible without impinging upon the rights guaranteed by the US Constitution and might even be detrimental to maintaining the US technological lead made possible by the free exchange of information. As compensation, Harold Brown suggested that US goals should be to keep the Soviets four or five years behind in militarily significant technologies (4:31).

The Soviets also use student and scientific exchanges to acquire technology. These exchanges are more pervasive when the political climate between the Soviet and US governments are cordial. At the height of detente in the 1970s, student exchanges were frequent and Soviet "students" were found studying advanced scientific subjects while their US counterparts were majoring in humanities (6:67). There are strong indications that these Soviet students were able to apply what they learned in the United States to develop advanced Soviet technologies.

Trade diversions have been extremely effective for the Soviets and have been on the rise (21:I-1). Through the formation of "front" companies or through the use of "third parties," the Soviets have been able to acquire advanced technology hardware for immediate application or reverse engineering (29:19). The challenge to ferret out legitimate from bogus companies in addition to identifying companies that disregard laws and agreements had been limited by resources. Because these operations are international, this method is difficult to control and can only be effectively countered by full COCOM cooperation.

The Federal Government's efforts to stem the tide of technology loss to the East has been hampered by interagency differences (14:14). Determination of what is militarily significant technology and which items should be granted export licenses because of foreign availability depends primarily on which agency's interest is at stake. Likewise, COCOM members have their own interests to protect and are very sensitive to perceived inconsistencies in US foreign policies.

Despite government shortfalls, there is evidence that the Reagan Administration's efforts to curb technology loss is working. Action taken include tougher export controls, agency reorganizations, funding increases, special operations, legal prosecutions, and frequent COCOM talks. An independent study known as the Aggregate Assessment showed that the Soviets would have saved $6.3-13.3 billion from 1985 to 1997, if they were allowed to acquire high technology found in 79 export items in the last two years (24:67). Additionally, increased cooperation by COCOM and friendly nations have resulted in a number of shipment seizures.

RECOMMENDATIONS

1. Central Organization. First of all, there needs to be unity of effort. The current method of Commerce granting export licenses after coordination with intelligence and DOD is an afterthought and a reaction to the realization that something quick needs to be done to stop the "hemorrhaging of technology." I recommend the creation of a central organization to deal with technology transfer. This organization needs to be at a level high enough to influence US policy. Since decisions on technology transfer affect foreign policy, national security, economic vitality, and freedom of information, an organization at a level lower than the cabinet will be brushed aside by entrenched parochial interests of other executive departments. A long-term solution is needed to deal with increasing complexities of issues like dual-use technology. This organization can deal with them.

Advantages. An organization whose mission is to control technology transfer can formulate a cohesive technology policy on student exchanges, bilateral agreements, and open source issues. It can coordinate with other agencies on how technology should be used in domestic, foreign, and trade policies. A more stable technology policy that does not reverse with each international incident is possible. Interagency squabblings on roles, responsibilities, and conflict of interests would be reduced. A more effective working relationship with intelligence and law enforcement agencies is possible because of the dedicated nature of the organization. It is also possible to be more consistent in working with COCOM.

Disadvantages. An effort to get the organization off the ground might detract from current efforts to counter technology transfer. Tremendous start-up obstacles can make the reality of such an organization unlikely. Political turf battles, costs, roles and responsibilities are but a few. Additionally, an organization dedicated to technology control could be myopic and ignore healthy trade for the sake of security.

2. COCOM Treaty. The United States needs to formalize COCOM with perhaps a treaty. COCOM must have more status and power to "reward the good and punish the bad." Nations intercepting illegal transfers should be rewarded and those that violate agreements need to be sanctioned. As an example, status similar to "most favored nation" could be the "carrot" and fines be the "stick." Technology must also be explicitly defined by the organization so that technology and not the product is controlled. A spirit of cooperation especially in sharing intelligence to predict what technology the Soviets are seeking should be encouraged. Effective control is impossible without COCOM cooperation.

COCOM needs to actively pursue technology-producing nations in the Third World to join the committee. Since so many of those nations now export dual-use technology, it is imperative that they do not out-compete US manufacturers observing unilateral domestic restraints. As COCOM grows in importance, it also needs to modernize through automation while maintaining the confidential atmosphere. Members should be asked to participate in economic burden-sharing of modernization with a system similar to that of NATO. Through these and other innovative steps, this can be a respected organization where technology-producing nations want to join. The United States should also exercise leverage (through policy application) linking progress in COCOM with the availability of US trade that individual nations need for their industries. In succinct terms, the United States should not give technology to nations that cannot protect it.

3. Industry Education Program. The government should work with industry in developing a program to educate high-tech industries on Soviet efforts to steal US technology. Include in the program a feedback system where industry becomes the ultimate source of control by reporting unusual orders. Commerce officials could periodically visit manufacturers to inspect their (proposed) technology transfer programs. Companies found in compliance of regulations are given favored licensing privileges, and those found in violation are given fines or other disincentives.

4. MCTL Update. The Militarily Critical Technologies List should be trimmed and periodically reviewed. New technology is constantly emerging and what was militarily significant a few years ago, might now be safely taken off the list. This list should not be allowed to stagnate or it will saturate the control system and prevent obsolete technology from being exported.

5. Security Clearance Review. A comprehensive review of security clearance recertification prodedures in the private sector needs to be done. Anyone working on sensitive programs should have their security clearances periodically reviewed. The Hughes employee who sold the look-down/shoot-down technology did not have his security clearance reviewed in 28 years (28:60).

6. Penalty Increases. Penalties for illegal shipments of high-tech and militarily significant hardware should be severe. Congress recently took positive steps by raising the maximum penalty to $1 million in fines and 10-year prison terms (21:I-1). In addition, violating companies should have their export licenses restricted.

7. NTIS Restriction. Prevent Soviet access to information on the Commerce Department's National Technical Information Service (NTIS) by restricting its content, labelling sensitive information as such, or put the information in other sources not accessible to the Soviets.

These recommendations, if implemented over time, offer some real disincentives to Soviet technology acquisition, while providing ample opportunity for American industry to continue its great history of leadership in technical development.

BIBLIOGRAPHY

A. REFERENCES CITED

Books

1. American Enterprise Institute. Proposals for Reforms of Export Controls for Advanced Technology. Washington DC: AEI Legislative Analysis, 1979.

2. Anning, N., D. Hebditch, and L. Melvern. Techno-Bandits. Boston: Houghton Mifflin Company, 1984.

3. Bertsch, Gary K., and John R. McIntyre (eds). National Security and Technology Transfer. Boulder, Colorado: Westview Press, 1983.

4. Brown, Harold. Thinking About National Security. Boulder, Colorado: Westview Press, 1983.

5. Godson, Roy (ed). Intelligence Requirements for the 1980's. Washington DC: National Strategy Information Center, Inc., 1980.

6. Laqueur, Walter. A World of Secrets. New York: Basic Books, Inc., 1985.

7. Parrott, Bruce (ed). Trade, Technology, and Soviet-American Relations. Bloomington: Indiana University Press, 1985.

8. Richelson, Jeffrey. Sword and Shield. Cambridge, Massachusetts: Ballinger Publishing Company, 1986.

9. -----. The U.S. Intelligence Community. Cambridge, Massachusetts: Ballinger Publishing Company, 1985.

10. Samli, A. C. (ed). Technology Transfer. Westport, Connecticut: Quorum Books, 1985.

11. Schaffer, Mark E. (ed). Technology Transfer and East-West Relations. New York: St. Martin's Press, 1985.

CONTINUED

12. Webster's New Collegiate Dictionary. Springfield, Massachusetts: G. & C. Merriam Company, 1976.

Articles and Periodicals

13. Asselin, Fred. "Technology Diversion." The Washington Quarterly, Vol. 7, No. 3 (Summer 1984), pp. 91-113, in Air War College Associate Programs Vol. I, Ch. 19, 19th ed., pp. 40-48.

14. Benson, Sumner. "Technology Security: Political Lessons for Public Managers." The Bureaucrat, Vol. 15, No. 2 (Summer 1986), pp. 7-10.

15. Burkhalter, E. A., Jr, Rear Adm, USN. "Soviet Industrial Espionage." Signal, Vol. 37, No. 7 (March 1983), pp. 15-20.

16. De Wolk, Roland. "U.S. Signs Soviets Off Computer." Oakland Tribune, 21 August 1986, p. 1.

17. Evans, Rowland, and Robert Novak. "Pentagon Sees Red Over Hi-tech Exports." New York Post, 30 Octoboer 1986, p. 20.

18. Farrar, Donald L. "Technology Transfer: Pros and Cons." Military Science and Technology, Vol. 4, No. 7 (July 1984), ICDM of North America, Inc., 1984, pp. 44-48, in Air War College Associate Programs Vol. I, Ch. 19, 19th ed., pp. 49-52.

19. Getz, Bill. "U.S. Says It Is Rooting Out Soviet Tech-spies." The Washington Times, 26 August 1986, p. 2.

20. Gross, Richard C. "TECHNOLOGY TRANSFER: Reversing The Tide." Defense Science & Electronics, Vol. 2, No. 1 (January 1983), pp. 11-17.

21. Kraul, Chris. "Illegal Export of Computer Components Commonplace." San Diego Union, 31 August 1986, p. I-1.

CONTINUED

22. Mann, Paul. "COCOM Agrees on Export of Computers." Aviation Week and Space Technology, Vol. 121, No. 4 (23 July 1984), pp. 21-22.

23. -----. "Smuggling Advances Soviet Technology." Aviation Week and Space Technology, Vol. 120, No. 15 (9 April 1984), pp. 24-25.

24. -----. "U.S. Tallies Cost to Soviets of Technology Transfer Rules." Aviation Week and Space Technology, Vol. 121, No. 24 (10 December 1984), pp. 67-69.

25. Perle, Richard N. "Technology Security, National Security, and U.S. Competitiveness." Science and Technology, (Fall 1986), p. 106, in Special Edition of Current News on Technology Security, No.1507, 30 October 1986, pp. 1-5.

26. Richardson, Michael. "US Plugging Loopholes, and Raising Hackles." Pacific Defence [sic] Reporter, Vol. 13, No. 2 (August 1986), pp. 32-33.

27. Thompson, Elvia H. "Technology Security: Administrative Challenge for Public Managers." The Bureaucrat, Vol. 15, No. 2, (Summer 1986), pp. 11-15.

28. Ulsamer, Edgar. "Moscow's Technology Parasites." Air Force Magazine, Vol. 67, No. 12 (December 1984), pp. 52-60.

29. Wohl, Richard. "Soviet Research and Development." Defense Science & Electronics, Vol. 2, No. 5 (September 1983), pp. 11-19.

30. Wu, Theodore W. "One on One." Defense News, Vol. 1, No. 32 (25 August 1986), p. 30.

Official Documents

31. US Superintendent of Documents. Soviet Military Power. Washington DC: Government Printing Office, 1986.

32. -----. Soviet Military Power. Washington DC: Government Printing Office, 1985.

33. -----. Soviet Military Power. Washington DC: Government Printing Office, 1984.

34. United States Congress, Office of Technology Assessment. Technology and East-West Trade: An Update. Washington DC: Government Printing Office, 1983.

B. RELATED SOURCES

Books

Liebrenz, Marilyn L. Transfer of Technology. New York: Praeger Publishers, 1982.

United States Congress, Office of Technology Assessment. Technology and East-West Trade. Monclair, New Jersey: Allanheld, Osmun/Gower & Company, 1981.

APPENDIX

CONVENTIONAL FORCE COMPARISONS

Conventional Force Comparisons: NATO and Warsaw Pact

		NATO				*Ratios of*	Warsaw Pact				
		Europe				*NATO/Pact*		Soviet		Non-Soviet	
		North[a]	South[b]	US	Total	*Totals*	Total	North[c]	South[d]	North[c]	South[d]
Manpower (000)											
Total uniformed manpower[e]		1,629	1,290	2,152	5,071	*1:1.27*	6,440	5,300		696	444
Reserves (all services)		2,200	2,312	2,332	6,844	*1:1.09*	7,484	5,400		1,181	903
Total ground forces		1,006	994	979	2,979	*1.06:1*	2,809	1,995		475	339
Total ground force reserves[f]		1,738	1,800	1,143	4,681*	*1:1.13*	5,280	3,500		995	785
Total ground forces deployed in Europe		877	994	217	2,088	*1:1.29*	2,685	1,173	698*	475	339
Divisions[g]											
Divs deployed in Europe, manned in peacetime	Tk[h]	12⅓	2	2⅓	16⅔	*1:1.60*	26⅔	14	2	8	2⅓
	Mech	5⅓	3	2⅓	10⅔	*1:4.13*	44	20	6	12	6
	Other	2⅓	1⅓	1⅓	5⅓	*1:1.35*	7⅓	3⅓	1⅓	2	1
Divs for reinforcement, manned or on mobilization of reserves[i]	Tk	6⅓	2⅓	4⅓	14	*1:2.21*	31	17	8	4	2
	Mech	14	17⅓	8⅓	40	*1:1.68*	67	18	29	5	15
	Other	13	17⅓	15⅓	46	–	–	–	–	–	–
Total divs, war mobilized[h]	Tk	19	4⅓	7	30⅓	*1:1.88*	57⅓	31	10	12	4⅓
	Mech	19⅓	20⅓	11	50⅓	*1:2.19*	111	38	35	17	21
	Other	15⅓	19⅓	16⅓	51⅓	*6.74:1*	7⅓	3⅓	1⅓	2	1
Ground Force Equipment											
Main battle tanks		8,799	6,534	5,000	20,333	*1:2.59*	52,600	24,200	13,800	10,200	4,400
Arty, MRL		4,235	4,509	670	9,414	*1:3.24*	30,500*	14,800	8,900	3,540	3,275*
SSM launchers		165	32	168	365	*1:4.30*	1,570	860	370	196	144
ATK guns		364	–	–	364	*1:4.63*	1,684*	456*	468	420	340*
ATGW launchers (crew-served, AFV-, hel-mounted)		1,292	134*	800*	2,226*	*1:2.79*	6,218*	2,660*	2,550*	688*	320
AA guns		3,776	1,778	100	5,654	*1:25.1*	4,506*[j]	1,100	780	1,576*	1,050
SAM launchers (crew-served, ground forces only)[k]		527	173	180	880	*1:6.60*	5,808*[j]	2,800*	1,730*	760*	518*

Source: The Military Balance 1985-1986, London, The International Institute for Strategic Studies, 1985, pp. 186-187.

Naval Units										
Submarines: cruise missile	–	–	–	–	–	41*	39	2	–	–
attack	87	48	53	188	*1.38:1*	136*	103	28*	3	2
Carriers	5	3	7	15	*5.00:1*	3	1	2	–	–
Cruisers	–	3	11	14	*11.79*	25	16	9	–	–
Destroyers	59	34	39	132	*2.49:1*	53*	31	21*	1	–
Frigates	98	40	47	185	*3.49:1*	53*	31*	15	2	5
Corvettes large patrol craft	68	52	–	120	*1.10:1*	125*	47*	30	33	15
FAC(G T P)	101	55	6	162	*1.2.36*	383*	110*	100	96	77
MCM[l]	185	77	3	265	*1.1.11*	293*	165*	65	50	13
Amphibious[m]	34	109	27	170	*1.75:1*	97	38	21	38	–
Naval and Maritime Aircraft										
Bombers	36	–	–	36	*1.5:1*	185	85	100	–	–
Attack	110	20	336	466	*3.61:1*	129*	30	65*	34	–
Fighters	44	8	168	220	*5.50:1*	40*	40*	–	–	–
ASW	21	6	70	97	*1.1.44*	140	140	–	–	–
MR ECM	160	49*	77	286	*1.80:1*	159*	99	50*	10	–
ASW hel	215	126	136	477	*4.30:1*	111	60	40	8	3
Land Attack Fighter Aircraft[n]										
Bombers	151	–	–	151	–	–	–	–	–	–
FGA	1,194	745	378	2,317	*1.1.23*	2,851*	1,915	325*	441	170
Fighters	94	216	144	454	*1.2.44*	1,110*	625*	265*	150	70*
Interceptors	351	–	96	447	*1.3.97*	1,775*	290*	265*	825	395
Reconnaissance[o]	195	93	69	357	*1.1.18*	423	167	80	110	66
Armed hel	(in Army)		330*		(data incomplete)	721*	495*	80*	102	44

* Estimated figures.

[a] Comprises Norway, Denmark, W. Germany, Luxembourg, Netherlands and Belgium, and includes forces actually deployed from Britain, Canada, US (Second Fleet), France (Army, Navy, Atlantic-deployed elms incl Naval air).

[b] Comprises Turkey, Greece, Italy, Portugal, France (Navy), US Sixth Fleet and forces deployed in Southern Europe.

[c] Comprises Poland, E. Germany and Czechoslovakia, and includes Soviet forces in those countries and in the Leningrad, Baltic, Byelorussian and Carpathian MD.

[d] Comprises Hungary, Romania and Bulgaria, and includes Soviet forces in Hungary and in the Odessa, Kiev, North Caucasus and Trans-Caucasus MD.

[e] 'Uniformed manpower' refers to main forces only and excludes para-military forces.

[f] 'Reserves'. Many countries have Reserve obligations into middle age, where not otherwise stated in the country entry, a five-year post-conscript period has arbitrarily been selected in calculating the numbers. After five years, health and training standards begin to decline. In Pact countries a large proportion of these older reservists are probably assigned to 'shadow' formations and units with stored obsolete equipment, potentially doubling the mobilizable forces from those shown but necessarily at very low standards of efficiency. The table, however, shows equipment totals for listed Category 1, 2 and 3 divisions only.

[g] Divisions are not a standard formation between Armies, 3 brigades or regiments are considered to be a divisional equivalent.

[h] 'Tk' includes tank and armoured divs, 'Mech' includes mechanized, motorized and motor rifle, 'Other' includes airborne, air portable, mountain, amphibious, light infantry and naval infantry.

[i] Mobilization and reserve reinforcement systems vary considerably. A distinction between the two categories of immediate reinforcement and 'when mobilized' must of necessity be judgmental, especially for NATO. This year's entry combines them, in contrast to previous years. See country entries for detail.

[j] Figures in part on unit organization. Ratio between guns and SAM may vary.

[k] Field forces only. Soviet Air Force and APVO equipment is considered primarily to be for airfield defence and not for use by field formations.

[l] Excludes support craft and inshore boats.

[m] Excludes LCV, LCVP, LCA, small craft.

[n] OCU aircraft are included in these totals.

[o] Includes EW, ECM aircraft.

END

5-87

DTIC